



IFW  
+  
\$

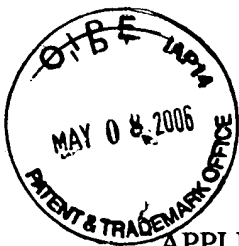
<b>TRANSMITTAL FORM</b> <i>(to be used for all correspondence during pendency of filed application)</i>		Application Number	10/698,814
		Filing Date	October 30, 2003
		First Named Inventor	Hugh S. Njemanze
		Group Art Unit Number	2161
		Examiner Name	Paul Kim
Total Number of Pages in This Submission	9*	Attorney Docket Number	25137-11333

ENCLOSURES (check all that apply)	
<input checked="" type="checkbox"/> Fee Transmittal Form (in duplicate) <input checked="" type="checkbox"/> Check Enclosed <input checked="" type="checkbox"/> Return Receipt Postcard <input type="checkbox"/> Response to Notice to File Missing Parts <input type="checkbox"/> Assignment & Recordation Cover Sheet <input type="checkbox"/> Declaration <input type="checkbox"/> Power of Attorney <input type="checkbox"/> Application Data Sheet <input checked="" type="checkbox"/> Information Disclosure Statement & PTO/SB/08A <input checked="" type="checkbox"/> Copies of IDS Cited Non-Patent References <input type="checkbox"/> Request for Corrected Filing Receipt <input type="checkbox"/> Request for Correction of Recorded Assignment <input type="checkbox"/> Amendment/Response: [ ] Page(s) <input type="checkbox"/> After Final <input type="checkbox"/> Status Request <input type="checkbox"/> Revocation and Substitute Power of Attorney	<input type="checkbox"/> Issue Fee Transmittal <input type="checkbox"/> Letter to Chief Draftsperson <input type="checkbox"/> Formal Drawing(s): [ ] Sheet(s) of Figure(s) [ ] <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input type="checkbox"/> Appeal Communication to Group (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> After Allowance Communication to Group <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
REMARKS: *Page count does not include cited references.	

SIGNATURE OF ATTORNEY OR AGENT			
Signature:			
Attorney/Reg. No.:	Sabra-Anne R. Truesdale, Reg. No. 55,687	Dated:	5-4-06

CERTIFICATE OF MAILING			
I hereby certify that this correspondence, including the enclosures identified above, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.			
Signature:			
Typed or Printed Name:	Sabra-Anne R. Truesdale	Dated:	5-4-06
Express Mail Mailing Number (optional):			





IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Hugh S. Njemanze  
APPLICATION NO.: 10/698,814  
FILING DATE: October 30, 2003  
TITLE: Expression Editor  
EXAMINER: Paul Kim  
GROUP ART UNIT: 2161  
ATTY. DKT. NO.: 25137-11333

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below:

Dated: 5-4-06

By: [Signature]  
Sabra-Anne R. Truesdale, Reg. No.: 55,687

MAIL STOP AMENDMENT  
COMMISSIONER FOR PATENTS  
P.O. BOX 1450  
ALEXANDRIA, VA 22313-1450

**INFORMATION DISCLOSURE STATEMENT**

**Under 37 CFR §§ 1.56 and 1.97-98**

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☐ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;

05/10/2006 WASFAW1 00000005 10698814

01 FC:1806

180.00 OP

25137/11333/DOCS/1617975.1

- ☒ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; or (2) an action that otherwise closes prosecution in the application, and:
  - ☒ attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(c); OR
  - ☐ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
    - ☐ no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to the knowledge of the person signing this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;
- ☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:
  - ☐ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;
    - ☐ no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to the knowledge of the person signing this


certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND

- ☐ attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(d); OR
- ☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.
- ☐ Enclosed is a copy of each listed reference that may be material to the examination of this application, and for which there may be a duty to disclose.
- ☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. \_\_\_\_\_, filed on \_\_\_\_\_, and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).
- ☒ Copies of any foreign patent documents and non-patent literature cited herein are enclosed.
- ☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in 37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).
- ☐ Applicant submits that no fee is required for the consideration of this Information Disclosure Statement.

Consideration of the listed references and favorable action are solicited.

Respectfully submitted,  
HUGH S. NJEMANZE

Dated: 5-4-06

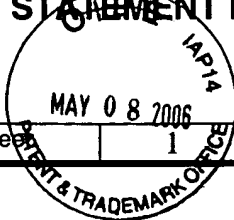
By:   
Sabra-Anne R. Truesdale, Reg. No.: 55,687  
Fenwick & West LLP  
Silicon Valley Center  
801 California Street  
Mountain View, CA 94041  
Tel.: (650) 335-7187  
Fax.: (650) 938-5200

# INFORMATION DISCLOSURE STATEMENT BY APPLICANT

## Complete if Known

Application No.	10/698,814
Filing Date	October 30, 2003
First Named Inventor	Hugh S. Njemanze
Art Unit	2161
Examiner Name	Paul Kim
Attorney Docket Number	25137-11333

Sheet 1 of 3



### U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No. <sup>1</sup>	Document No. Number – Kind Code <sup>2</sup> (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	A1	US-2004/0221191 A1	11-04-2004	Porras et al.
	A2	US-6,711,615	03-23-2004	Porras et al.
	A3	US-6,708,212	03-16-2004	Porras et al.
	A4	US-6,704,874 B1	03-09-2004	Porras et al.
	A5	US-2004/0024864 A1	02-05-2004	Porras et al.
	A6	US-2004/0010718 A1	01-15-2004	Porras et al.
	A7	US-2003/0093514 A1	05-15-2003	Valdes et al.
	A8	US-2003/0093692 A1	05-15-2003	Porras
	A9	US-2003/0101358 A1	05-29-2003	Porras et al.
	A10	US-6,484,203	11-19-2002	Porras et al.
	A11	US-6,321,338	11-20-2001	Porras et al.
	A12	US-5,717,919	02-10-1998	Kodavalla et al.

### FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No. <sup>1</sup>	Foreign Patent Document Country Code <sup>3</sup> – Number <sup>4</sup> Kind Code <sup>5</sup> (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T <sup>6</sup>

### OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T <sup>6</sup>
	C1	ARCSIGHT, "About ArcSight Team," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/about_team.htm">http://www.arcsight.com/about_team.htm</a> >.	
	C2	ARCSIGHT, "About Overview," October 14, 2002, [online] [Retrieved on April 21, 2006] Retrieved from the Internet <URL: <a href="http://web.archive.org/web/20021014041614/http://www.arcsight.com/about.htm">http://web.archive.org/web/20021014041614/http://www.arcsight.com/about.htm</a> >.	
	C3	ARCSIGHT, "Contact Info," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/contact.htm">http://www.arcsight.com/contact.htm</a> >.	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609.

Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup>Applicant's unique citation designation number (optional). <sup>2</sup>See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT****Complete if Known**

Application No.	10/698,814
Filing Date	October 30, 2003
First Named Inventor	Hugh S. Njemanze
Art Unit	2161
Examiner Name	Paul Kim
Attorney Docket Number	25137-11333

Sheet 2 of 3

**OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T <sup>6</sup>
	C4	ARCSIGHT, "Enterprise Coverage: Technology Architecture," date unknown, [online] Retrieved from the Internet <URL: <a href="http://www.snaiso.com/Documentation/Arcsight/arcsight_archdta.pdf">http://www.snaiso.com/Documentation/Arcsight/arcsight_archdta.pdf</a> >.	
	C5	ARCSIGHT, "Managed Process: ArcSight Reporting System," date unknown, [online] Retrieved from the Internet <URL: <a href="http://www.snaiso.com/Documentation/Arcsight/arcsight_reportsys.pdf">http://www.snaiso.com/Documentation/Arcsight/arcsight_reportsys.pdf</a> >.	
	C6	ARCSIGHT, "Managed Process: Console-Based Management," date unknown, [online] Retrieved from the Internet <URL: <a href="http://www.snaiso.com/Documentation/Arcsight/arcsight_console.pdf">http://www.snaiso.com/Documentation/Arcsight/arcsight_console.pdf</a> >.	
	C7	ARCSIGHT, "Precision Intelligence: SmartRules™ and Cross-Correlation," date unknown, [online] Retrieved from the Internet <URL: <a href="http://www.snaiso.com/Documentation/Arcsight/arcsight_correlation.pdf">http://www.snaiso.com/Documentation/Arcsight/arcsight_correlation.pdf</a> >.	
	C8	ARCSIGHT, "Precision Intelligence: SmartAgent™," date unknown, [online] Retrieved from the Internet <URL: <a href="http://www.ossmanagement.com/SmartAgent.pdf">http://www.ossmanagement.com/SmartAgent.pdf</a> >.	
	C9	ARCSIGHT, "Product Info: Product Overview and Architecture," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product.htm">http://www.arcsight.com/product.htm</a> >.	
	C10	ARCSIGHT, "Product Info: 360° Intelligence Yields Precision Risk Management," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info01.htm">http://www.arcsight.com/product_info01.htm</a> >.	
	C11	ARCSIGHT, "Product Info: ArcSight SmartAgents," October 10, 2002, [online] [Retrieved on April 21, 2006] Retrieved from the Internet <URL: <a href="http://web.archive.org/web/20021010135236/http://www.arcsight.com/product_info02.htm">http://web.archive.org/web/20021010135236/http://www.arcsight.com/product_info02.htm</a> >.	
	C12	ARCSIGHT, "Product Info: ArcSight Cross-Device Correlation," date unknown, [online] [Retrieved on October 25, 2005] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info03.htm">http://www.arcsight.com/product_info03.htm</a> >.	
	C13	ARCSIGHT, "Product Info: ArcSight Manager," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info04.htm">http://www.arcsight.com/product_info04.htm</a> >.	
	C14	ARCSIGHT, "Product Info: ArcSight Console," date unknown, [online] [Retrieved on November 15, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info05.htm">http://www.arcsight.com/product_info05.htm</a> >.	
	C15	ARCSIGHT, "Product Info: ArcSight Reporting System," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info06.htm">http://www.arcsight.com/product_info06.htm</a> >.	
	C16	ARCSIGHT, "Product Info: Enterprise Scaling," date unknown, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/product_info07.htm">http://www.arcsight.com/product_info07.htm</a> >.	
	C17	ARCSIGHT, "Security Management for the Enterprise," 2002, [online] [Retrieved on October 25, 2002] Retrieved from the Internet <URL: <a href="http://www.arcsight.com/">http://www.arcsight.com/</a> >.	
	C18	ARCSIGHT, "Technical Brief: How Correlation Eliminates False Positives," date unknown, source unknown.	
	C19	BURLESON, D., "Taking Advantage of Object Partitioning in Oracle8i," November 8, 2000, [online] [Retrieved on April 20, 2004] Retrieved from the Internet <URL: <a href="http://www.dba-oracle.com/art_partit.htm">http://www.dba-oracle.com/art_partit.htm</a> >.	
	C20	DERODEFF, C. "Got Correlation? Not Without Normalization," 2002, [online] Retrieved from the Internet <URL: >.	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609.

Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup>Applicant's unique citation designation number (optional). <sup>2</sup>See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT****Complete if Known**

Application No.	10/698,814
Filing Date	October 30, 2003
First Named Inventor	Hugh S. Njemanze
Art Unit	2161
Examiner Name	Paul Kim
Attorney Docket Number	25137-11333

Sheet	3	of	3
-------	---	----	---

**OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T <sup>6</sup>
		<a href="http://www.svic.com/papers/pdf/Got-Correlation_rmalization.pdf">http://www.svic.com/papers/pdf/Got-Correlation_rmalization.pdf</a> .	
	C21	CHEUNG, S. et al., "EMERALD Intrusion Incident Report: 601 Message Specification," August 10, 2000, System Design Laboratory, SRI International.	
	C22	National Institute of Standards and Technology (NIST), "Federal Information Processing Standards Publication (FIPS PUB) 199: Standards for Security Categorization of Federal Information and Information Systems", February 2004.	
	C23	Haley Enterprise, "Production Systems," 2002, [online] [Retrieved on October 29, 2002] Retrieved from the Internet <URL: <a href="http://www.haley.com/0072567836705810/ProductionSystems.html">http://www.haley.com/0072567836705810/ProductionSystems.html</a> >.	
	C24	Haley Enterprise, "The Rete Algorithm," 2002, [online] [Retrieved on October 29, 2002] Retrieved from the Internet <URL: <a href="http://www.haley.com/0072567836705810/ReteAlgorithm.html">http://www.haley.com/0072567836705810/ReteAlgorithm.html</a> >.	
	C25	Haley Enterprise, "A Rules Engine for Java Based on the Rete Algorithm," 2002, [online] [Retrieved on October 29, 2002] Retrieved from the Internet <URL: <a href="http://www.haley.com/0072567836705810/ReteAlgorithmForRules.html">http://www.haley.com/0072567836705810/ReteAlgorithmForRules.html</a> >.	
	C26	HALME, L.R. et al., "AINT Misbehaving: A Taxonomy of Anti-Intrusion Techniques," 2000, [online] [Retrieved on November 1, 2002] Retrieved from the Internet <URL: <a href="http://www.sans.org/newlook/resources/IDFAQ/aint.htm">http://www.sans.org/newlook/resources/IDFAQ/aint.htm</a> >.	
	C27	LINDQVIST, U. et al., "Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST)," Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 1999.	
	C28	CERT Coordination Center, "Overview of Attack Trends," 2002, [online] Retrieved from the Internet <URL: <a href="http://www.cert.org/archive/pdf/attack_trends.pdf">http://www.cert.org/archive/pdf/attack_trends.pdf</a> >.	
	C29	PORRAS, P.A. et al., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," October 1997, Proceedings of the 20 <sup>th</sup> NIST-NCSC National Information Systems Security (NISS) Conference.	
	C30	PORRAS, P.A. et al., "A Mission-Impact-Based Approach to INFOSEC Alarm Correlation," October 2002, Lecture Notes in Computer Science, Proceedings: Recent Advances in Intrusion Detection, pp. 95-114, Zurich, Switzerland.	
	C31	INGARGIOLA, G., "The Rete Algorithm," date unknown, [online] [Retrieved on October 29, 2002] Retrieved from the Internet <URL: <a href="http://yoda.cis.temple.edu:8080/UGAIWWW/lectures/rete.html">http://yoda.cis.temple.edu:8080/UGAIWWW/lectures/rete.html</a> >.	
	C32	BRUNEAU, G., "What Difficulties are Associated on Matching Events with Attacks. Why is Event/Data Correlation Important?," 2001, [online] [Retrieved on November 1, 2002] Retrieved from the Internet <URL: <a href="http://www.sans.org/newlook/resources/IDFAQ/matching.htm">http://www.sans.org/newlook/resources/IDFAQ/matching.htm</a> >.	
	C33	National Institutes of Health (NIH), "Table 1: Security Categorization of Federal Information and Information Systems," revised July 8, 2005, [online] [retrieved on April 6, 2006] Retrieved from the Internet <URL: <a href="http://irm.cit.nih.gov/security/table1.htm">http://irm.cit.nih.gov/security/table1.htm</a> >.	
	C34	WOOD, M., et al., "Internet-Draft: Intrusion Detection Message Exchange Requirements," June 23, 2002, [online] [Retrieved on November 1, 2002] Retrieved from the Internet <URL: <a href="http://www.silicondefense.com/idwg/draft-ietf-idwg-requirements-07.txt">http://www.silicondefense.com/idwg/draft-ietf-idwg-requirements-07.txt</a> >.	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609.

Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup>Applicant's unique citation designation number (optional). <sup>2</sup>See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.